IN THE CLAIMS:

Please AMEND claims 1, 3, 5, 7-15, and 20;

Please ADD claims 22-38; and

Please CANCEL claims 6, 19, and 21 without prejudice or disclaimer, as shown below.

1. (Currently Amended) A system, comprising:

a mobile node belonging to a home network located within a secure network, the mobile node having a network interface configured to communicate with other nodes, the mobile node having only one security association and only one mobility binding with a home agent so as to provide secure mobile connectivity that implements a mobile internet protocol home agent functionality;

a proxy home agent connected to the home network and located within the secure network, wherein the proxy home agent is configured to provide a proxying functionality;

the home agent located outside of the secure network, wherein the home agent is configured to provide a signaling and tunneling functionality and to notify the proxy home agent of the mobile node;

a virtual private network gateway located outside the secure network and configured to work in conjunction with the home agent; and

a demilitarized zone located outside the secure network, wherein the virtual private network gateway and the home agent reside in the demilitarized zone;

a first firewall between the secure network and the demilitarized zone,

wherein the mobile node has a permanent address in a known range and the first firewall is programmed to deny all communications from the demilitarized zone with a source address in the known range, and

wherein the virtual private network gateway has a direct connection to an internal interface of the first firewall such that the first firewall considers the virtual private network gateway transmitted data as internal to the secure network.

2. (Previously Presented) The system of claim 1, wherein the virtual private network gateway and the home agent are located within a single device within a demilitarized zone.

3. (Currently Amended) The system of claim 1, wherein~~further comprising~~ the~~a~~ first firewall is coupled to the secure network and the virtual private network gateway, wherein the home agent is located within the first firewall.

4. (Previously Presented) The system of claim 1, wherein the home agent is a separate device from the virtual private network gateway.

5. (Currently Amended) The system of~~according to~~ claim 1, further comprising:

a second firewall between the demilitarized zone and an external network configured to deny communications from the external network with a source address in the known range~~,~~

~~wherein the mobile node has a permanent address in a known range~~.

6. (Cancelled)

7. (Currently Amended) The system of claim 1, wherein~~further comprising:~~ the~~a~~ demilitarized zone comprises~~ing~~ a first router ~~coupled to a second router~~ that is coupled to the~~a~~ first firewall, the virtual protocol network gateway coupled to the first router~~,~~ and the first firewall, wherein the home agent is coupled to the first router, and wherein the demilitarized zone is coupled to a second router.

8. (Currently Amended) The system of claim 7, wherein packets from the mobile node destined toward nodes inside the secure network first go the home agent and then to the virtual protocol network gateway that is configured to forward the packets through the first firewall to the secure network.

9. (Currently Amended) The system of claim 8, wherein packets from the second router to the first firewall having a source address in the~~a~~ known range are dropped by the first firewall.

10. (Currently Amended) The system of~~according to~~ claim 1, wherein a router is directly connected to the~~a~~ first firewall, and the virtual protocol network gateway and the home agent are configured to connect to a different interface of the router and the first firewall.

11. (Currently Amended) The system of claim 10, wherein the first firewall is configured such that it considers the interface with which it connects to the virtual protocol network gateway as an internal interface and packets with a source address that are outside of a known address range received on the internal interface are dropped, and packets with a source address that are within the known address range that are received by the first firewall on an external interface are dropped.

12. (Currently Amended) The system of claim 11, wherein virtual protocol network encapsulated packets are forwarded to the virtual protocol network gateway and when a security association exists, the packet is decrypted and forwarded to the first firewall on the internal interface and when the~~a~~ security association does not exist the packet is dropped.

13. (Currently Amended) The system of claim 12, wherein mobile internet protocol packets and virtual protocol network encapsulated packets first reach the home agent which are forwarded to the virtual protocol network gateway and then to the secure network through the first firewall's internal interface.

14. (Currently Amended) The system of claim 1, wherein~~further comprising:~~ the~~a~~ first firewall coupled to the secure network and the virtual protocol network gateway,~~;~~ and further comprising:

a router comprising an access control list used to drop packets that have a source address that belong to a known address range.

15. (Currently Amended) A method, comprising:

~~establishing a proxy home agent located within the secure network to~~ monitoring data directed to a~~the~~ mobile node so as to secure communication between the~~a~~ mobile node associated with a home network in a secure network and a correspondent node;

~~establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node;~~

collecting data directed to the mobile node;

~~packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual protocol network packaged data; and~~

~~tunneling the virtual protocol network packaged data to a current address of the mobile node; and~~

packaging the collected data in an internet-protocol-in-internet-protocol tunnel; and

sending the packaged data~~it~~ to a virtual protocol network gateway~~device~~ for virtual protocol network encryption, wherein the encrypted data is packaged in a virtual protocol network secure tunnel to a permanent address, located in the secure network, of the mobile node to create virtual protocol network packaged data that is~~and~~ tunnel~~ed~~ing ~~the virtual protocol network packaged data~~ to a~~the~~ current address of the mobile node.

16. (Previously Presented) The method of claim 15, wherein the virtual protocol network secure tunnel follows the internet protocol security protocol.

17. (Previously Presented) The method of claim 15, wherein the tunneling of the virtual protocol network packaged data to the external mobile node occurs according to the internet protocol mobility protocol.

18-19 (Cancelled)

20. (Currently Amended) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

~~establishing a proxy home agent located within a secure network to~~ monitoring data directed to a mobile node so as to secure communication between the mobile node associated with a home network in a secure network and a correspondent node;

~~establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node;~~

collecting data directed to the mobile node;

~~packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual private network packaged data;~~

~~tunneling the virtual private network packaged data to a current address of the mobile node; and~~

packaging the collected data in an internet-protocol-in-internet-protocol tunnel; and

sending the packaged data~~it~~ to a virtual protocol network gateway~~device~~ for virtual protocol network encryption, wherein the encrypted data is packaged in a virtual protocol network secure tunnel to a permanent address, located in the secure network, of the mobile node to create virtual protocol network packaged data that is~~and~~ tunnel~~ed~~ing ~~the virtual protocol network packaged data~~ to a~~the~~ current address of the mobile node.

21. (Cancelled)

22. (New) The method of claim 15, further comprising:

creating or removing a proxy address resolution protocol entry for a permanent address associated with the mobile node.

23. (New) An apparatus, comprising:

a processor configured to monitor data directed to a mobile node so as to secure communication between the mobile node associated with a home network in a secure network and a correspondent node;

a receiver configured to collect data directed to the mobile node,

wherein the processor is configured to package the collected data in an internet-protocol-in-internet-protocol tunnel; and

a transmitter configured to send the packaged data to a virtual protocol network gateway for virtual protocol network encryption, wherein the encrypted data is packaged in a virtual protocol network secure tunnel to a permanent address, located in the secure network, of the mobile node to create virtual protocol network packaged data that is tunneled to a current address of the mobile node.

24. (New) The apparatus of claim 23, wherein the virtual protocol network secure tunnel follows the internet protocol security protocol.

25. (New) The apparatus of claim 23, wherein the virtual protocol network packaged data is tunneled to the external mobile node according to the internet protocol mobility protocol.

26. (New) The apparatus of claim 23, wherein the processor is configured to create or remove a proxy address resolution protocol entry for a permanent address associated with the mobile node.

27. (New) An apparatus, comprising:

a processor configured to create only one security association with a mobile node associated with a home network in a secure network and only one mobility binding with the mobile node; and

a transmitter configured to notify a proxy home agent located within the secure network of the mobile node,

wherein the processor is configured to tunnel virtual protocol network packaged data to a current address of the mobile node.

28. (New) The apparatus of claim 27, wherein the transmitter is configured to communicate to the proxy home agent that the mobile node has moved outside the home network.

29. (New) The apparatus of claim 28, wherein the transmitter is configured to communicate to the proxy home agent that the mobile node has come back to the home network.

30. (New) An method, comprising:

creating only one security association with a mobile node associated with a home network in a secure network and only one mobility binding with the mobile node;

notifying a proxy home agent located within the secure network of the mobile node; and

tunneling virtual protocol network packaged data to a current address of the mobile node.

31. (New) The method of claim 30, further comprising:

communicating to the proxy home agent that the mobile node has moved outside the home network.

32. (New) The method of claim 31, further comprising:

communicating to the proxy home agent that the mobile node has come back to the home network.

33. (New) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

creating only one security association with a mobile node associated with a home network in a secure network and only one mobility binding with the mobile node;

notifying a proxy home agent located within the secure network of the mobile node; and

tunneling virtual protocol network packaged data to a current address of the mobile node.

34. (New) An apparatus, comprising:

a receiver configured to receive collected data from a proxy home agent; and

a processor configured to encrypt the collected data, wherein

the processor is configured to package the encrypted data in a virtual private network secure tunnel to a permanent address, located in a secure network, of a mobile node to create virtual protocol network packaged data that is tunneled to a current address of the mobile node.

35. (New) The apparatus of claim 34, wherein the virtual private network secure tunnel includes an encapsulating security payload field comprising information regarding security used.

36. (New) A method, comprising:

receiving collected data from a proxy home agent;

encrypting the collected data; and

packaging the encrypted data in a virtual private network secure tunnel to a permanent address, located in a secure network, of a mobile node to create virtual protocol network packaged data that is tunneled to a current address of the mobile node.

37. (New) The method of claim 36, wherein the virtual private network secure tunnel includes an encapsulating security payload field comprising information regarding security used.

38. (New) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

receiving collected data from a proxy home agent;

encrypting the collected data; and

packaging the encrypted data in a virtual private network secure tunnel to a permanent address, located in a secure network, of a mobile node to create virtual protocol network packaged data that is tunneled to a current address of the mobile node.